



Amazon  
Linux

# Administración de archivos de registro



# INTRODUCCIÓN

La administración de archivos de registro (logs) es una parte esencial de la gestión de sistemas en Linux. Los archivos de registro contienen información crucial sobre las actividades del sistema, errores, eventos de seguridad y el comportamiento de las aplicaciones. Un manejo eficiente de estos archivos permite a los administradores de sistemas supervisar la salud del sistema, diagnosticar y solucionar problemas, y mantener la seguridad.

## OBJETIVOS

- Revisar lastlog y los resultados de registro seguros de la máquina de Linux



# TAREA 1

En esta tarea, se conectará a una instancia EC2 de Amazon Linux. Utilizará una utilidad SSH para realizar todas estas operaciones. Las siguientes instrucciones varían ligeramente según si utiliza Windows o Mac/Linux.

## En Linux

- o Usando distribución Ubuntu con Subsistema de Windows para Linux (WSL).

```
ec2-user@ip-10-0-10-43:~ x + v
leps2408@LAPTOP-1I89QL1A:~$ neofetch
./+oossssoo+/- .
`:+ssssssssssssssssst+:`
-+ssssssssssssssssssyyssst+-
.ossssssssssssssssssdMMMMNyssssso.
/ssssoosssssshdmmNNmmyNNMMhssssso/
+sssoosssssshmydMMMMMMNdddyssssso+
/ssssoosssshNNMMYhhyyyyhmNNMMNhssssso/
.ssssoossssdMMMNhssssssssshNNMMdssssso.
+sssoohhhyNNMMNysssssssssssyNNMMYssssso+
ossyNNMMNyMMhssssssssssshmmhssssso
ossyNNMMNyMMhssssssssssshmmhssssso
+sssoohhhyNNMMNysssssssssssyNNMMYssssso+
.ssssoossssdMMMNhssssssssshNNMMdssssso.
/ssssoosssshNNMMYhhyyyyhdNNMMNhssssso/
+sssoossssdmydMMMMMMNdddyssssso+
/ssssoosssshdmmNNNNmmyNNMMhssssso/
.ossssssssssssssssssdMMMMNyssssso.
-+ssssssssssssssssssyyssst+-
`:+ssssssssssssssssst+:`
./+oossssoo+/- .

leps2408@LAPTOP-1I89QL1A
-----
OS: Ubuntu 20.04.6 LTS on Windows 10 x86_64
Kernel: 5.15.153.1-microsoft-standard-WSL2
Uptime: secs
Packages: 673 (dpkg), 4 (snap)
Shell: bash 5.0.17
Theme: Adwaita [GTK3]
Icons: Adwaita [GTK3]
Terminal: Relay(482)
CPU: Intel i5-10300H (8) @ 2.496GHz
GPU: 0929:00:00.0 Microsoft Corporation Device 008e
Memory: 421MiB / 3838MiB
```





## TAREA 2

En esta tarea, utilice herramientas comunes de Linux para revisar los archivos de registro seguros y utilice la aplicación *lastlog* de Linux para revisar los inicios de sesión anteriores.

- o Comprobar que se encuentra en la carpeta CompanyA.

```
ec2-user@ip-10-0-10-132:~/cc x + v
[ec2-user@ip-10-0-10-132 ~]$ pwd
/home/ec2-user
[ec2-user@ip-10-0-10-132 ~]$ ls
companyA
[ec2-user@ip-10-0-10-132 ~]$ cd companyA/
[ec2-user@ip-10-0-10-132 companyA]$ |
```

- o Para usar el archivo de registro seguro como prueba, ingresar *sudo less /tmp/log/secure*.

```
ec2-user@ip-10-0-10-132:~/cc x + v
Aug 23 03:47:13 centos7 sshd[3283]: Invalid user guest from 193.201.224.218
Aug 23 03:47:13 centos7 sshd[3283]: input_userauth_request: invalid user guest [preauth]
Aug 23 03:47:13 centos7 sshd[3283]: pam_unix(sshd:auth): check pass; user unknown
Aug 23 03:47:13 centos7 sshd[3283]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=
ssh ruser= rhost=193.201.224.218
Aug 23 03:47:15 centos7 sshd[3283]: Failed password for invalid user guest from 193.201.224.218 port 13181
ssh2
Aug 23 03:47:16 centos7 sshd[3283]: pam_unix(sshd:auth): check pass; user unknown
Aug 23 03:47:17 centos7 sshd[3283]: Failed password for invalid user guest from 193.201.224.218 port 13181
ssh2
Aug 23 03:47:18 centos7 sshd[3283]: pam_unix(sshd:auth): check pass; user unknown
Aug 23 03:47:20 centos7 sshd[3283]: Failed password for invalid user guest from 193.201.224.218 port 13181
ssh2
Aug 23 03:47:24 centos7 sshd[3283]: pam_unix(sshd:auth): check pass; user unknown
Aug 23 03:47:25 centos7 sshd[3283]: Failed password for invalid user guest from 193.201.224.218 port 13181
ssh2
Aug 23 03:47:26 centos7 sshd[3283]: pam_unix(sshd:auth): check pass; user unknown
Aug 23 03:47:27 centos7 sshd[3283]: Failed password for invalid user guest from 193.201.224.218 port 13181
ssh2
Aug 23 03:47:27 centos7 sshd[3283]: pam_unix(sshd:auth): check pass; user unknown
Aug 23 03:47:29 centos7 sshd[3283]: Failed password for invalid user guest from 193.201.224.218 port 13181
ssh2
Aug 23 03:47:29 centos7 sshd[3283]: Disconnecting: Too many authentication failures for guest [preauth]
Aug 23 03:47:13 centos7 sshd[3283]: Invalid user guest from 193.201.224.218
Aug 23 03:52:40 centos7 sshd[5160]: Invalid user acc from 193.201.224.218
Aug 23 03:52:45 centos7 sshd[5243]: Invalid user adam from 193.201.224.218
Aug 23 03:52:53 centos7 sshd[5312]: Invalid user adfexc from 193.201.224.218
Aug 23 03:53:45 centos7 sshd[5494]: Invalid user admin2 from 193.201.224.218
Aug 23 03:53:45 centos7 sshd[5494]: pam_unix(sudo:session): session opened for user root by (uid=0)
:|
```



- o Ingresar *sudo lastlog*, para ver la hora del último inicio de sesión de todos los usuarios en la máquina.

```
ec2-user@ip-10-0-10-132:~/cc x + v
[ec2-user@ip-10-0-10-132 companyA]$ sudo lastlog
Username      Port      From      Latest
root          **Never  logged in**
bin           **Never  logged in**
daemon       **Never  logged in**
adm          **Never  logged in**
lp           **Never  logged in**
sync         **Never  logged in**
shutdown     **Never  logged in**
halt         **Never  logged in**
mail         **Never  logged in**
operator     **Never  logged in**
games        **Never  logged in**
ftp          **Never  logged in**
nobody       **Never  logged in**
systemd-network
dbus         **Never  logged in**
rpc          **Never  logged in**
libstoragemgmt
sshd         **Never  logged in**
rngd         **Never  logged in**
rpcuser      **Never  logged in**
nfsnobody    **Never  logged in**
ec2-instance-connect
postfix      **Never  logged in**
chrony       **Never  logged in**
tcpdump      **Never  logged in**
ec2-user     pts/0    190.234.179.212 Thu Aug 1 03:30:41 +0000 2024
ljuan        **Never  logged in**
mmajor       **Never  logged in**

```



## Desafío adicional

¿Qué información se puede extraer para algunos de los propósitos de su empresa?

- o La información del comando last puede proporcionar varios insights útiles para la administración del sistema y la seguridad en una empresa. Principalmente, muestra los usuarios asociados y cuando ingresaron.